PAR 22

UNCLASSIFIED

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

ANAS ELHADY, et al.,	)	
Plaintiffs,	)	
v.	)	Case No. 1:16-cv-375
CHARLES H. KABLE, et al.	)	
Defendants.	)	

DECLARATION OF MICHAEL A. CHRISTMAN
FEDERAL BUREAU OF INVESTIGATION

I, Scott A. Rago, hereby declare as follows, pursuant to 28 U.S.C. § 1746:

1. I am the Acting Deputy Assistant Director ("DAD") of the Operational Programs Branch ("OPB"), Criminal Justice Information Services Division ("CJIS"), Federal Bureau of Investigation ("FBI"), United States Department of Justice. Aside from my role as Acting DAD, I am the Section Chief of the Global Law Enforcement Support Section ("GLESS"), which is within OPB. I was designated as the Section Chief of GLESS in January 2019. Prior to that time, I had served as Section Chief of the Global Operations Section beginning in 2016. I began my career as a Special Agent with the FBI in 2000. As the Acting DAD of OPB, I oversee a number of the CJIS Division's programs and initiatives, including the National Crime Information Center ("NCIC"), a nationwide, computerized information system and the CJIS Audit Unit.

2. I submit this declaration in support of the motion for summary judgment being filed by Defendants. I understand that, within the FBI, separate declarations from the Terrorist

Screening Center, the Counterterrorism Division, and the CJIS Division's National Instant Criminal Background Check System ("NICS") Section, are being submitted concurrently. This declaration addresses the ability to search the NCIC, a nationwide, computerized information system, which contains, among other files, the Known or Suspected Terrorist ("KST") File, which is populated with a subset of TSDB information. The FBI, through the CJIS Division, functions as the national manager for the NCIC.

3. The statements contained in this declaration are based upon my personal knowledge, upon information provided to me in my official capacity, and upon conclusions and determinations reached and made in accordance therewith.

4. Title 28, United States Code ("U.S.C."), Section 534, authorizes the United States Attorney General to acquire, collect, classify, and preserve identification, criminal identification, crime, and other records. The authority and power vested in the United States Attorney General to perform these functions has been delegated to the FBI by Title 28, Code of Federal Regulations ("C.F.R."), Section 0.85(b). Regulations governing the NCIC are found at 28 C.F.R., Part 20.

5. Consistent with these authorities, the NCIC links criminal justice and law enforcement agencies in the fifty states, the District of Columbia, U.S. Territories, and Canada. Generally speaking, the function of the NCIC is to assist the criminal justice community by providing information to apprehend fugitives, locate missing persons, locate and return stolen property, or other similar criminal justice objectives.

6. The NCIC consists of 21 files. As stated above, among these is the KST File.[1] This file, which is a subset of the TSDB, is exported by the TSC to the NCIC. Inclusion of the KST File in the NCIC allows for federal, state, and local law enforcement and criminal justice agencies to share relevant information necessary to carry out their respective missions in a concerted effort to prevent terrorist attacks. Users access information in the NCIC Files by entering name, date of birth, or social security number. A user cannot perform a search if only a name is entered.

7. NCIC terminals are in effect computers. The FBI does not provide terminals or hardware. Terminals or other hardware devices access NCIC through a regional and/or state/federal computer system. The FBI provides a host computer and telecommunication lines to a single point of contact in each of the 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, and Canada, as well as federal criminal justice agencies. That single point of contact is the state CJIS Systems Agency ("CSA"), which is typically the state's lead criminal justice agency, which is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include all local levels. Those CSA jurisdictions, in turn, operate their own telecommunications systems, providing access to nearly all local criminal justice agencies and authorized non-criminal justice agencies nationwide.

---

1. In addition to the KST File, the NCIC includes 13 other person files, including: Supervised Release; National Sex Offender Registry; Foreign Fugitive; Immigration Violator; Missing Person; Protection Order; Unidentified Person; Protective Interest; Gang; Wanted Person; Identity Theft; Violent Person; and NICS Denied Transaction. The NCIC also includes 7 property files containing records of stolen articles, boats, guns, license plates, parts, securities, and vehicles. The system also contains a limited capability to associate images with NCIC records to help agencies identify people and property items.

8. Within the CSA is an individual CJIS Systems Officer ("CSO") who is responsible for the administration of the CJIS network for the CSA. The purpose behind a designated state CSO within the CSA is to consolidate responsibility for ensuring compliance by all ORI users with established procedures and policies within each signatory state agency.

9. In order for an entity to search information in the NCIC, the entity must apply for and obtain an Originating Agency Identifier ("ORI")[2] from the CJIS Division. A governmental law enforcement or criminal justice agency's request to the CJIS Division for an ORI assignment must be accompanied by, among other things: documentation demonstrating that the agency was established pursuant to executive order, statute, or ordinance; documentation of its arrest powers or criminal justice functions, as also outlined via executive order, statute, or ordinance; and documentation that more than fifty percent of its budget is allocated to the administration of criminal justice functions, as defined in 28 C.F.R. § 20.3(b).

10. Because some law enforcement or criminal justice agencies may enter into agreements with private entities to assist in carrying out their criminal justice mission, federal regulations allow NCIC information to be made available to certain private entities, subject to strict oversight and control. In order for a private entity to obtain an ORI that provides NCIC access, that entity must be providing services for the administration of criminal justice in accordance with 28 C.F.R. § 20.33(a)(7).[3] Likewise, Congress has recognized that qualified

---

2. An ORI is a multi-character alphanumeric identifier assigned by NCIC to an agency or entity in order to identify it in transactions on the NCIC System.

3. The federal regulations, at 28 C.F.R. § 20.20, indicate that information from NCIC is subject to the limitations contained in 28 C.F.R. § 20.33(a)(7), which fall under subpart C of 28 C.F.R. Part 20. Section 20.20(a) states, in part: "Use of information obtained from the FBI Identification Division [the precursor to the CJIS Division] or the FBI/NCIC system shall also be subject to limitations contained in subpart C.")

police departments of railroads or private colleges or universities can gain NCIC access pursuant to 28 U.S.C. § 534(e).

11. The types of non-governmental entities with NCIC access under 28 C.F.R. § 20.33(a)(7) include: private correctional facilities; private security services for governmental facilities and hospitals; entities providing criminal justice dispatching services or data processing/information services to governmental criminal justice agencies; private probation and pretrial services entities; private city attorneys; and other entities similarly performing criminal justice services. These other entities are: a private police department for an airport; a private police department for a transportation authority; private police departments for two private incorporated communities; law enforcement divisions of certain Societies for the Prevention of Cruelty to Animals ("SPCAs"); an inmate transport service; an entity that provides forensic services to detect and identify criminals; and court constable services.

12. Those entities that are authorized to access NCIC pursuant to 28 C.F.R. § 20.33(a)(7) may only access NCIC pursuant to an agreement with a governmental law enforcement or criminal justice agency (CJA), or with a noncriminal justice governmental agency performing criminal justice dispatching services or data processing/information services for a governmental criminal justice agency. The private entity is, thus, providing services on behalf of or in support of a CJA. NCIC can only be searched for criminal justice purposes or pursuant to a federal statute, and thus cannot generally be searched by a private entity (or, any entity with NCIC access, for that matter) as part of a civil background check. For example, a police department at a college or a hospital cannot use NCIC to screen school applicants, students, hospital patients or visitors, as that is not a criminal justice purpose.

13. A private entity's request to the CJIS Division for an ORI must be submitted by the governmental agency with whom the private entity has an agreement. And before that request even reaches the CJIS Division, the state CSO must first review it and determine whether the private entity is eligible for an ORI. The CSO also makes a determination regarding whether the assignment of an ORI is appropriate and warranted under the specific circumstances. If the state CSO agrees with the request for an ORI, only then does the state CSO pass that request along to the CJIS Division. The CJIS Division does not accept requests directly from private entities; they must apply through the CJA they are working with, and via the state CSO.

14. A private entity's request for an ORI must be accompanied by a description of the criminal justice duties (as defined at 28 CFR, § 20.3(b)) that the private entity will be performing on behalf of the governmental entity as well as a copy of the required agreement between a governmental CJA and the private entity, including the contract's executed signature page(s). The agreement must incorporate the FBI CJIS Security Addendum. The agreement must also specify a representative from the CJA that will assume NCIC operational responsibility and agree to act as the Agency Coordinator ("AC"). The AC manages the agreement between the private entity and the governmental agency. The tasks of the AC include responsibility for supervision and ensuring the integrity of the NCIC system by requiring training, continuing education, and certification testing of all personnel who have or will have access to the NCIC system.

15. Pursuant to 28 C.F.R. § 20.33(a)(7), the agreement between the private contractor and the governmental agency must incorporate a security addendum approved by the Attorney General of the United States, which limits the use of the NCIC information, ensures the security and confidentiality of the information consistent with regulations and CJIS security policies,

provides for sanctions, and contains such other provisions as the Attorney General may require. The power and authority of the Attorney General under this provision is exercised by the FBI Director (or the Director's designee). The CJIS Security Addendum, found at Appendix H to the CJIS Security Policy[4], is the uniform addendum to an agreement between the governmental agency and a private contractor, approved by the Attorney General, which contains the provisions required under 28 C.F.R. § 20.33(a)(7).

16. Private entities who perform criminal justice functions must meet the same training and certification criteria required by governmental agencies performing a similar function, and are subject to the same audit review as are law enforcement user agencies. All personnel at the private entity who perform criminal justice functions are required to acknowledge, by signing the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. Police departments of railroads and private colleges or universities that obtain NCIC access pursuant to 28 U.S.C. § 534(a) must also comply with the CJIS Security Policy. In order to qualify for an ORI, railroad police departments and the police departments of private colleges and universities must (1) "perform the administration of criminal justice and have arrest powers pursuant to a State statute," (2) "allocate a substantial part of their annual budget to the administration of criminal justice," and (3) "meet training requirements established by law or ordinance for law enforcement officers."

---

4. The CJIS Security Policy, found at https://www.fbi.gov/file-repository/cjis-security-policy_v5-7_20180816.pdf/view, provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of criminal justice information. The CJIS Security Policy provides that data contained in CJIS systems, including data in the NCIC, is sensitive information and security must be afforded to prevent any unauthorized access, use, or dissemination of the information. Improper access, use, or dissemination of NCIC information is serious and may result in the imposition of administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

17. The CJIS Security Policy has strict security protocols for accessing the NCIC. NCIC is not web-based and is not available or accessible on the internet. It is a machine-to-machine interface. A user, whether at a law enforcement or criminal justice agency or an authorized private entity, accesses NCIC through the CSA's network, using the ORI and other identifiers. Every NCIC user must undergo an FBI fingerprint background check prior to being authorized to access NCIC.

18. On a biennial basis, the state/federal CSA is responsible for validating the criminal justice, law enforcement, or other valid basis for access, and all information contained within each field of the ORI File for every agency accessing the CJIS Division systems. If an entity merged or changed names, the state/federal CSA is required to gather the appropriate documentation from the entity. The state/federal CSA then forwards it to the CJIS Division for review. Depending on the documentation, the ORI information could be modified or retired if the documentation no longer supported the qualifications under 28 U.S.C. § 534 or 28 C.F.R., Part 20. Depending on the circumstance, an existing ORI may need to be retired and a new ORI issued.

19. If, for example, a college or university has a private security service but then changes the company providing that service, then the college or security service notifies the state CSA of the change, and the state CSA contacts CJIS to retire the ORI and provide the new request for a new ORI to CJIS. A new ORI would be issued to the new private security service, so long as a new agreement is in place and all other requirements are met for ORI eligibility. The same process would take place if an agreement expires or is not renewed according to the specific terms of a particular agreement.

20. Governmental agencies and private entities with an ORI are subject to auditing. The state CSA is required to audit every agency and entity with an ORI within the state on a triennial basis. In addition, the state CSA must have the technical means to log every transaction that comes through the state CSA. The CJIS Security Policy requires the CSA to have a protocol in place to regularly review those logs, in order to detect unusual or suspicious behavior. The FBI's CJIS Audit Unit also audits every CSA, as well as a selection of agencies and/or entities, on a triennial basis.

21. During a CJIS audit of a CSA, CJIS physically visits the CSA. Ahead of the visit, CJIS collects information and requires the CSA to complete a lengthy questionnaire that covers the security requirements set forth in the CJIS Security Policy. CJIS auditors review the answers with the CSO during the visit, to determine whether and how the CSA is complying with the security requirements. The areas of focus during the CJIS Audit include: where the information is kept, who has access, and how the CSA is preventing both unauthorized access as well as improper use by authorized users. The CJIS audit covers many aspects of security, even delving into things such as how NCIC print outs are shredded, the type of virus detection software being used, any firewalls being used, the user system itself, user names and passwords, and intrusion detection. It also reviews whether every user in the state has been fingerprinted and undergone a FBI fingerprint background check, whether they've been trained, the policies in place, how those policies are shared, and how users are made aware of them. In addition to auditing the CSA, CJIS also picks a random sampling of several governmental agencies within the state to audit. These agencies are also required to complete a lengthy questionnaire and are subject to detailed review by CJIS. CJIS also asks these agencies whether and how the CSA is complying with security requirements. If CJIS suspects any misuse, it informs the CSA, so the CSA can further

investigate and take any necessary and appropriate action. During the state CSA's audit, similar reviews are conducted of user agencies and entities.

22. Each user agency is required to have its own policy regarding misuse and discipline for such misuse. For those private entities in an agreement with a CJA, that CJA is responsible for the private users' searches of NCIC and use of any information returned.

23. Under 28 C.F.R. § 20.38, the FBI CJIS Division can cancel an ORI, effectively revoking NCIC access, if misuse is identified. A state CSA can do the same if it finds wrongdoing. Typically, however, when the CJIS Division finds a misuse or a concern, the state CSO cooperates with efforts to identify the misuse, correct it, and report back to CJIS regarding corrective measures. Individual users within an agency or entity have been disciplined, including termination from employment, and can also face federal criminal charges for misuse or unauthorized use of a government computer system or government property.

24. The FBI previously identified 1441 ORIs issued to private entities pursuant to either 28 C.F.R. § 20.33 or 28 U.S.C. § 534. Subsequently, after accounting for duplicate entries and eliminating a number of city attorneys that, upon further review, were determined to be governmental entities, the FBI approximated that the number of qualified private entities to which ORIs have been issued was approximately 533. As explained, the number of private entities issued ORIs under these provisions required de-duplication because in many cases multiple ORIs have been issued to the same entity. An entity may have numerous ORIs assigned when the entity or agency has a need to identify internal divisions, units, substations, or multiple terminals for the same agency within the same city. In addition, if an entity resides in and uses NCIC in multiple cities or states, ORIs may be assigned for each location. A qualifying private entity is not granted multiple ORIs unless it demonstrates a need to distinguish NCIC

transactions by separate internal divisions, units, or substations, or that it conducts its criminal justice services in multiple locations and requests multiple ORIs.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this __th day of March 2019.

Scott A. Rago
Acting Deputy Assistant Director
Operational Programs Branch
Criminal Justice Information Services Division
Federal Bureau of Investigation